



**Comments of the
World Shipping Council**

**Before the
United States Coast Guard**

**In the matter of
Maritime Security Temporary Interim Rules**

**Docket Numbers:
USCG-2003-14792
USCG-2003-14733
USCG-2003-14749
USCG-2003-14732
USCG-2003-14757**

July 31, 2003

I. Introduction

The World Shipping Council (“the Council” or “we”) submits these comments¹ in response to the six temporary interim rules issued by the United States Coast Guard (“Coast Guard”) on July 1, 2003 (68 Fed.Reg. 39240 et seq.). In these rules, the Coast Guard solicited comments on its plans for complying with the requirements of the Maritime Transportation Security Act of 2002 (MTSA) and the maritime security requirements set forth in the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code and amendments to the International Convention for the Safety of Life at Sea (SOLAS). These interim rules address: 1) Implementation of National Maritime Security Initiatives, 2) Area Maritime Security, 3) Vessel Security, 4) Facility Security, 5) Outer Continental Shelf Facility Security, and 6) Automatic Identification System; Vessel Carriage Requirements.

The Council appreciates the opportunity to provide comments to the Coast Guard on its interim regulations for complying with the MTSA, ISPS Code and SOLAS requirements. The Council, a non-profit association of over forty international ocean carriers, was established to address public policy issues of interest and importance to the international liner shipping industry. The Council’s members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry more than 93% of the United States’ imports and exports transported by the international liner shipping industry, or roughly \$500 billion worth of American foreign commerce per year.²

International liner shipping provides regular, scheduled services connecting U.S. exporters and importers with virtually every country in the world. Liner shipping vessels make more than 22,000 calls at ports in the United States each year or more than 60 vessel calls a day. The Coast Guard temporary interim rules discussed herein, as well as the requirements in the ISPS Code and SOLAS amendments, set forth security requirements on international vessels that operate in U.S. waters. To that end, our industry has supported the Coast Guard in its role as the lead U.S. agency responsible for ensuring the safety and security of vessels that call upon, and interface with, U.S. ports and facilities.

The Council commends the U.S. Coast Guard for its efforts to quickly establish comprehensive, meaningful, and harmonized domestic and international security standards for ships and port facilities. The Coast Guard deserves credit for simultaneously and successfully partnering with domestic and international industry stakeholders, the IMO, other federal agencies and the U.S. Congress. The implementation of the ISPS Code and SOLAS amendments, which the Coast Guard helped develop through international agreement, is very important not only to enhance maritime security, but also to create a consistent, uniform international approach for our industry, which operates within the jurisdiction of all the maritime trading nations of the world. We believe that the Coast Guard’s efforts in this regard serve as a model for future regulatory endeavors because its approach sought consistency and predictability amongst and between

¹ The Council also endorses the comments jointly submitted in this matter by the United States Maritime Alliance, the National Association of Waterfront Employers, and the Pacific Maritime Association.

² A list of the Council’s members is attached as Appendix A.

domestic and international requirements. We recognize, however, that implementation of these maritime security regulations will require considerable time and resources on the part of the Coast Guard, other governments, and the industry.

The Council appreciates the opportunity to continue to work with the Coast Guard and other U.S. federal agencies to develop maritime security requirements that enhance security without unnecessarily impacting the movement of commerce to and from the United States. We offer these comments in support of the Coast Guard's effort to promulgate regulations to implement the requirements of the MTSA, the SOLAS amendments, and the ISPS Code. This comment submission will address each of the six regulation packages in order as promulgated in the Federal Register, with the exception of part 106, "Outer Continental Shelf Facility Security." At the beginning of each comment, the title, parts (under 33 CFR Subchapter H), docket number and section of each interim rule will be listed, where applicable.

II. Implementation of National Maritime Security Initiatives (Part 101) (Docket Number: USCG-2003-14792)

Purpose (Section 101.100):

The Council commends the Coast Guard for the opening section of this interim rule. The Coast Guard has been highly focused and diligent in advocating enhanced vessel and port facility security through the International Maritime Organization (IMO). Its extensive efforts were instrumental in producing the new ISPS Code and the maritime security amendments to the SOLAS Convention. Because of the extensive cooperation that other maritime nations agreed to provide in agreeing to these IMO requirements, it is wholly appropriate that the Coast Guard acknowledge the alignment of these interim rules with the agreements that the United States government successfully negotiated at the IMO last December, and reinforce the strong interest in ensuring that international security arrangements are compatible and mutually consistent.

Federal Preemption of State and Local Laws

The Council very strongly supports the interim regulations' preemption of state regulations on the issues addressed by the Coast Guard in these initiatives. We fully support the statements made at 68 Fed. Reg. 39277 stating that the federalism principles enunciated in *U.S. v. Locke* regarding preemption of state laws apply to the Coast Guard's maritime security regulation and control of vessels, as well as its security regulation of ports and facilities.

The Coast Guard's preemption statement is especially critical with respect to vessels on international voyages, because the success of the entire international regime, with which the Coast Guard has wisely chosen to make U.S. regulations consistent, requires that operators of international vessels be able to meet the laws of all countries by adopting and following a single vessel security plan. The preemption statement by the Coast Guard will not only prevent the creation of a patchwork quilt of state and local laws in the U.S., but also sends an important

message to the governments of U.S. trading partners that the United States speaks with one voice on issues of maritime security.

The Coast Guard is also correct that state laws would cause either actual conflicts or conflicts with an over-riding need for federal uniformity. There is an additional conflict as well – a conflict in resource allocation. Even where there was not a direct conflict between federal and state or local law (i.e., where it was technically possible to comply with both simultaneously), a requirement to comply with two regulatory regimes would divert scarce resources that are necessary for prompt compliance with the federal regime. Given the anticipated costs of many of the measures required, this financial conflict is as real as any technical or legal conflict.

The United States Supreme Court has consistently held that federal action in the area of maritime regulation preempts state law. In the *Locke* case cited by the Coast Guard, for example, the Court had the following to say in striking down state regulations on tank vessels: “The existence of the treaties and agreements on standards of shipping is of relevance, of course, for those agreements give force to the longstanding rule that the enactment of a uniform federal scheme displaces state law, and the treaties indicate Congress will have demanded national uniformity regarding maritime commerce.” Especially where, as is the case here, the federal regulation is so closely intertwined with an international regime in which the U.S. participates, there is simply no room for state regulations.

Coordination With Customs and Border Protection

As discussed above, the Coast Guard has developed a credible security regime, with international cooperation, for vessels and port facilities. At the same time, Customs and Border Protection (CBP) has developed a credible security strategy and set of regulations, with international cooperation, for containerized cargo security. The Coast Guard and CBP are sister agencies within the Department of Homeland Security (DHS). It is critically important that the two agencies enter into a Memorandum of Understanding (MOU) outlining appropriate roles and responsibilities with regard to port, vessel and cargo security, as soon as possible. The Coast Guard and CBP have acknowledged in writing, during public meetings, and in Congressional testimony their agencies’ differing but complementary maritime security roles—the Coast Guard serving as the lead agency in port and vessel security, and CBP serving as the lead agency in cargo security. An MOU would demonstrate that the agencies within DHS are prepared and in agreement regarding roles, procedures and responsibilities for dealing with a maritime security question that may arise regarding containerized cargo. Past experience illustrates that such an MOU is needed. Carriers, their customers, and the public have a legitimate expectation that the responsible federal agencies have a clear and agreed set of protocols defining roles, responsibilities and coordination. An MOU would clarify the roles of the Coast Guard and CBP for other agencies within DHS, the U.S. government, the Congress, as well as the governments of our foreign trading partners. The Council urges the Coast Guard and CBP to enter into a maritime security MOU as soon as possible. The Council has made the identical request of CBP.

Recognized Security Organization (RSO) Competencies

Part B of the ISPS Code, includes a list of competencies on which RSOs are to be evaluated by flag states wishing to use RSOs to evaluate vessel and facility security assessments and plans. In the supplemental discussion preceding the regulations section of this interim rule (68 Fed.Reg. 39254), the Coast Guard states that the list of RSO competencies provided in the ISPS Code, part B, encompasses the essential qualifications and competencies of organizations that wish to assist the maritime industry in the development of their security assessments and plans. We support the Coast Guard's declaration in this regard and wish to point out that high-quality RSOs will play an important and necessary role in assisting other flag administrations manage the massive task of assessing and approving hundreds of vessel security plans and assessments and issuing International Ship Security Certificates (ISSC) by July 1, 2004. Many RSOs will be reputable security organizations, associations or classification societies that have valuable expertise, adhere to high standards of quality and service to the maritime industry, and to which the Coast Guard has awarded its high ratings on its Port State Control website.

The Council understands that the Coast Guard intends to monitor individual RSOs by tracking their vessels' maritime security detention rates and other performance factors, with a view to using this data as a key factor in determining what Port State Control actions will be applied to each vessel. The Council supports the Coast Guard's plan to use its Port State Control program to ensure that vessel security assessments, plans and ISSCs approved by designated RSOs comply with the requirements of the ISPS Code and SOLAS amendments. In this regard, we recommend that the Coast Guard make its RSO evaluation processes and findings as transparent as possible by publishing on the Coast Guard Port State Control website the list of RSOs that the Coast Guard has evaluated and the relative performance ratings of each evaluated RSO.

Preparedness Communications, Attainment (Section 101.300 (c))

This provision requires vessel and facility owners and operators to confirm to the local Coast Guard Captain of the Port (COTP) their attainment of measures or actions required in their security plans upon notification of a change in the MARSEC level. While we understand and appreciate the Coast Guard's desire to monitor the security status of each vessel and facility within each COTP region, we recommend that the Coast Guard not require vessel and facility owners and operators to make notifications to the COTP of measures or actions already outlined in their respective security plans. First, making attainment reports to specify that a vessel or facility is operating in accordance with its security plan appears to be redundant and adds no apparent security value. The basic principle on which the security plan was designed is that the security measures in the plan will be adjusted based on the MARSEC level of the location in which the vessel or facility is located. This means that vessels and facilities are required to adjust their security measures to comply with the changing MARSEC levels. Notifying the Coast Guard that they have attained the measures required by their plan would create extensive administrative requirements with little or no apparent security value.

Furthermore, for international liner vessels that call on multiple U.S. ports on a regular schedule, this attainment notification requirement would mandate multiple, redundant calls to

many COTP regions each week. The time spent making such notifications would appear to be better spent implementing security measures. Another concern with regard to making attainment notifications is that it is not clear what the Coast Guard would do with this information, nor is it clear how vessel and facility owners and operators would be expected to perform such notifications. Would each COTP region attempt to track the MARSEC readiness of all facilities and vessels in its area of operations with a view to contacting those vessels and facilities that have not filed attainment notifications? Given the huge number of diverse vessels that call a given COTP region in the course of one day, it would appear that tracking the attainment reporting of all vessels in a COTP region would be a time and resource consuming exercise. As to the issue of how to perform these attainment notifications, there has been no guidance regarding a consistent, reasonable, and timely way for making such notifications, if they were required. Of major concern to the Council is the need for consistency and uniformity from COTP region to region. Vessels, in particular, would have additional difficulty complying with an attainment notification requirement if the vessel had to make such notifications by different means or procedures and to different entities within each COTP region.

For these reasons, the Council recommends that the Coast Guard eliminate the requirement for attainment notifications and instead use spot inspections to verify that vessels and facilities are implementing the security measures detailed in their security plans.

Additional Communication Devices (Section 101.310)

As stated in section 101.300, paragraphs (a) and (b), (entitled, *Notification of MARSEC Level Change and Communication of Threats*) the COTP will communicate changes in MARSEC levels and appropriate threat information to port stakeholders, vessels and facilities through a local Broadcast Notice to Mariners and a Maritime Security Directive, or as detailed in the Area Maritime Security (AMS) Plan. The Coast Guard has also indicated that it intends to communicate changes in the national MARSEC level to U.S. ports and vessels operating in U.S. waters using public alert systems, Broadcast Notice to Mariners, fax and e-mail alert lists and other similar methods, and will use the toll-free National Response Center as its point of contact. Given the advent of low-cost, advanced and highly reliable communications systems, we recommend that the Coast Guard consider alternative means, in addition to or in place of the Broadcast Notice to Mariners and other manual means, for disseminating changes in MARSEC levels and threat information to the industry. To that end, we strongly encourage the Coast Guard to develop a uniform national system for communicating MARSEC changes and threat information quickly and efficiently to vessels, facilities and port stakeholders. Potential solutions that we recommend the Coast Guard explore include:

- 1) Communication Of Local MARSEC Levels And Appropriate Threat Information On The National Response Center (NRC) Website. The NRC is currently recognized by the maritime industry as the Coast Guard's primary center for collecting reports of suspicious activities, potential terrorist acts and oil spills. We recommend that the NRC website be used as the primary means of communicating MARSEC levels changes and threat information for all COTP regions throughout the U.S. and for collecting reports of suspicious maritime homeland security information from the maritime community. By keeping this website updated with all changes to COTP MARSEC levels, and by providing access to general,

localized threat information on the site, the Coast Guard could provide “one-stop shopping” to the maritime community for critical maritime security information. The confusion as to what the MARSEC level is in each COTP region would be alleviated because the MARSEC levels for all COTP regions would be available on one website. Use of such a system might also reduce the number of phone calls and emails to Coast Guard staff assigned to each COTP office, as the industry would learn to rely on the website as the primary system for disseminating and collecting maritime security information. Under this system, vessels enroute to specific U.S. ports of discharge or their agents could either check the website using onboard communications systems (if available), receive MARSEC information from shore-based agents by email, fax, VHF radio-telephone or mobile phone, or simply listen for the Broadcast Notice To Mariners.

2) Notice Of Arrival (NOA) Return Receipt Message: Another communication mechanism would be for the Coast Guard to communicate the current MARSEC level in the anticipated port of arrival and provide general, localized threat information via an electronic return receipt email message sent back to the vessel upon receipt of the NOA. Currently NOA information is communicated electronically from the vessel via email or fax to the Coast Guard National Vessel Movement Center 96 hours before arrival of the vessel. Upon receipt of an NOA message from a vessel bound for a U.S. port, the Coast Guard could simply send an automated response email to the vessel indicating the MARSEC level in the intended port of arrival as well as providing generalized local threat information.

3) Automatic Identification System (AIS) Messages: Another alternative would be to communicate MARSEC levels and localized threat information to the inbound vessel via the Automatic Identification System (AIS), once that system is fully operational. One of the benefits of AIS is that it will provide two-way communications capabilities that could enable the Coast Guard to proactively disseminate changes in MARSEC levels and threat information directly to all AIS vessels within a certain range.

Finally, we recommend that the Coast Guard consider establishing the ability to communicate individualized threat information to specific vessels, classes of vessels, vessel lines, or vessels bound to or from specific ports, rather than relying only on generic threat communication capability to the entire industry. We believe that receipt of this targeted, localized and ship-specific threat information would enhance the readiness of the maritime industry to respond.

MARSEC Directives (Section 101.405)

This provision states that the Commandant of the Coast Guard or his delegee may issue MARSEC Directives when the Coast Guard determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against the U.S. maritime transportation system. The section also states that all MARSEC Directives will be issued as Sensitive Security Information (SSI) and that affected vessel and facility owners and operators will be advised via the Federal Register to travel to their local COTP or Coast Guard District Commander to pick up a paper copy of the MARSEC Directive. Before being issued a copy of the directive, owners and operators will be required to prove that they have “a need to know”,

that they are a “covered person” and that they have SSI clearance authority as defined by 49 CFR 1520. Owners and operators to whom a MARSEC Directive applies must then, in a separate action, acknowledge receipt of the directive, comply with the directive, and within the prescribed timeframe notify the Coast Guard of the specific methods by which the security measures have been implemented.

The Council supports the Coast Guard’s intended use of MARSEC Directives as means for communicating critical, timely threat information and for mandating additional security measures in the event of an known terrorist threat. The above processes for receiving and complying with these directives, however, are cumbersome and bureaucratic and fail to take advantage of the efficiency of modern communication systems to quickly and securely disseminate threat information and mandate additional security measures.

The Council urges the Coast Guard to identify a better means of quickly communicating MARSEC Directives to vessel, port and facility owners and operators. Earlier in these comments, we suggested that the Coast Guard utilize the NRC website as the single location for disseminating MARSEC levels and localized threat information for all COTP regions and for collecting reports of suspected terrorist activity. Similarly, we recommend that the Coast Guard utilize the NRC website as the primary conduit for communicating MARSEC Directives to the maritime industry. To ensure that the threat information is protected as SSI, the information could be provided via a secure web-interface in which designated vessel and facility owners and operators are issued a username and password after having been cleared for access to SSI. The Coast Guard could also maintain a national email database of all vetted, SSI cleared vessel and facility owners and operators, and upon issuance of a MARSEC Directive, the Coast Guard could send an urgent email notification advising each owner or operator to log into the NRC website to download the MARSEC Directive.

Until a web-based system can be developed for disseminating MARSEC Directives—and we urge the Coast Guard to develop such a system as soon as practicable—we suggest the Coast Guard alter the manual process for disseminating MARSEC directives outlined in the interim regulations as follows:

- 1) Acknowledgment of Receipt: When a vessel or facility owner or operator picks up the copy of the MARSEC directive from the Coast Guard, he should not be required at a later time to acknowledge receipt of it. The owner or operator instead should simply sign for the document at the time of pick up.
- 2) Notification That Additional Security Measures Have Been Implemented: The vessel or facility owner or operator should not be required to notify the Coast Guard that it has implemented the security measures mandated by the MARSEC Directive. We do not see the need for owners and operators to make notifications to the Coast Guard advising that they have implemented the additional security measures specified in the MARSEC directive, because, 1) each vessel and facility owner, upon receipt of a MARSEC Directive has an affirmative understanding that the measures in the directive are to be implemented immediately, 2) the approved security plan would be expected to provide for the necessary flexibility and comprehensiveness to readily implement required countermeasures, and 3) making such notifications takes away from time that could

better be spent implementing security measures. Consistent with the arguments discussed in the attainment notification comments above, we recommend that the Coast Guard issue the MARSEC Directive and then verify compliance by using spot inspections. The vessel or facility owner or operator should also not be required to communicate to the Coast Guard the specific countermeasures he has employed to comply with the directive. The regulations do not specify by what means such notification to the Coast Guard is to be made, but presumably such communications would rely on non-secure means and would effectively compromise the SSI contained in the MARSEC Directive as well as the security countermeasures that were implemented by the vessel or facility, thus making the countermeasures easier to defeat or circumvent. Furthermore, the time spent reporting the details of additional security measures employed could more effectively be spent deploying those measures. Finally, the reporting requirements of this section are of concern because they would mandate the reporting of hundreds of simultaneous phone, fax and email notifications to each Coast Guard COTP advising that vessel and facility owners and operators are complying with the MARSEC directive. This would appear to be very burdensome to the Coast Guard and could impair the reporting of critical information on threats, vessels in distress or other emergencies.

Sensitive Security Information

The supplemental discussion preceding Part 101 of this interim rule, states in part that, in order to ensure that dissemination of maritime security material does not make the vessel, facility or port vulnerable to a transportation security incident, the Coast Guard has included provisions in these interim rules indicating that vessel and facility security material is to be designated as Security Sensitive Information (SSI) in accordance with 49 C.F.R. Part 1520. The Council supports the Coast Guard's plans to apply an appropriate security designation to vessel and facility security material. The interim rule does not, however, specify the process whereby specific industry officials, such as vessel and facility owners, operators, security officers and security personnel, may apply for and receive clearances to gain access SSI material from the Coast Guard.

Our initial understanding of the Coast Guard's SSI access authorization process is that local COTPs will have the authority to designate specific individuals, within their area of operations, who are authorized access to Coast Guard generated SSI material. If this is a correct depiction of the SSI access authorization process, we believe that such a process would create significant difficulties for liner vessel owners and operators, VSOs and other shipboard security personnel, because liner vessels call on multiple U.S. ports during a single voyage. For example, under the SSI access authorization process described above in which each COTP could develop unique SSI application requirements, a vessel master and VSO on a single vessel could be required to make multiple, redundant applications for SSI clearances to every COTP region in which the vessel operates. This SSI access authorization process would unnecessarily burden shipboard security personnel and would also appear to be burdensome on the Coast Guard, because it would duplicate efforts through the processing and issuance of multiple SSI clearances to a single individual. We recommend that the Coast Guard establish a uniform national SSI access authorization program through which shipboard security personnel may apply for SSI clearances

through a single COTP and, once granted, have access to SSI material on a need to know basis, in any COTP region.

Seafarers' Identification Criteria Requirements (Section 101.515)

The Supplementary Information to the Temporary Interim Rule on Implementation of National Maritime Security Initiatives (68 Fed.Reg. 39240 et seq.) discusses the various provisions in the MTSA pertaining to crewmember credentialing and the development of a transportation security card for access to secure areas on a vessel or a facility. Recognizing that the Transportation Security Administration is in the process of developing a Transportation Worker Identification Card (TWIC) to satisfy the latter MTSA requirement, the Council would like to offer some comments regarding those provisions of the MTSA that we understand have been delegated to the Coast Guard by a delegation of authorities from the Secretary of Homeland Security. They are 46 U.S.C. 70111 and MTSA Section 103.

46 U.S.C. 70111 authorizes the Secretary, in consultation with the Attorney General and the Secretary of State, to require crewmembers on vessels calling at U.S. ports to carry, and present on demand, "any identification that the Secretary decides is necessary". The provision also authorizes the Secretary, again in consultation with the Attorney General and the Secretary of State, to establish "the proper forms and process that shall be used for identification and verification of crew members".

The Coast Guard has determined that identification forms, which meet the requirements in the agency's earlier notice on "Maritime Identification Credentials" (67 Fed.Reg. 51082 et seq.), will continue to be acceptable as meeting the statutory requirement mentioned above. The requirements for acceptable identification forms have been incorporated in the Temporary Interim Rule at 33 CFR § 101.515.

The Council supports, and agrees with, the Coast Guard's determination. We do so with the understanding that also so-called "seamen's books" and other flag-state issued mariner's documents, including STWC certificates, will continue to be acceptable forms of identification even though such flag-state issued documents may not always be laminated.

However, the discussion in the Supplementary Information also indicates that the Coast Guard will be assessing the utility of the recently completed negotiations at the International Labor Organization (ILO) on a new Convention on Seafarers' Identity Documents.³

We recognize that time constraints prevented the Coast Guard from discussing the possible implications of the new ILO Convention for the implementation of the MTSA's requirements on seafarer identification. We also recognize that other U.S. government agencies are responsible for setting U.S. government policies on aspects of the potential use of the new identification

³ "Because this interim rule has been published in a timeframe that did not allow us to incorporate the results of the ILO conference into it, we will issue any further requirements pertaining to seafarer identification under a separate rulemaking, if appropriate". 68 Fed.Reg. 39264. The new ILO convention that revises the existing ILO Seafarers' Identity Documents Convention from 1958 (which the United States did not ratify), is accessible at: www.ilo.org/public/english/standards/relm/ilc/ilc91/pdf/pr-20a.pdf

document. At the same time, however, the Coast Guard was involved in negotiating the ILO agreement, and will presumably be involved in determining and explaining the use of this new document.

We would urge the Coast Guard to provide a comprehensive and clear explanation of the usages U.S. government agencies with responsibilities in regard to foreign seafarers will make of the new ILO seafarers' identity documents. First, it is important to know if the ILO document will serve any role in the visa application process or in facilitating the travel of the seafarer to and from the United States, and if so what role that would be. We are not aware of any such role, and in fact understand that the document will have no such role.⁴ Second, if the new ILO document's purpose is only to serve as personal identification, then some persons may perceive the new document as being just another bureaucratic layer without meaningful, added use and value. If foreign seafarers are required to obtain individual visas, including the requirement of a personal interview by a consular officer, in order to be allowed to leave the vessel in a U.S. port to repatriate (or be allowed to be in transit to join a vessel in a U.S. port), and the new ILO document plays no facilitation role in obtaining such a visa or in their admission to the United States, the value of the new document would be unclear and significant disappointment to many. Third, if the new ILO document is to be considered as a required document for seafarers, we would like to know why seafarers with U.S. visas would need to have such documents in addition to their passports, and we would like to know if this means that all U.S. merchant mariner documents would have to be reissued in a manner that is consistent with the ILO document's parameters.

During the ILO negotiations, the United States government expressed support for the development of a new international seafarers' identification document, which – through the incorporation of biometric identifiers, the inclusion of personal data and electronic access to such data residing in databases in the issuing country and elsewhere – would make it possible to verify the identity, employment history and credentials of a foreign seafarer, including for visa application purposes.

This objective of developing an instrument that would provide for an identification form that could be used also in the visa application process was explicitly included in the U.S. government's response to a questionnaire by the ILO Secretariat in preparation for the final negotiation rounds. In its response to one of the questions in the ILO questionnaire⁵, the U.S. government stated that U.S. immigration laws require a foreign seafarer to hold a valid visa unless U.S. border agents waive this requirement. The response then continued: "The United States Government does, however, support the principle that a new seafarer identification document, including biometric identifiers, should to the maximum extent possible be designed so that it contains, or provides direct electronic access to, information elements needed to initiate the visa application process where applicable".

⁴ The U.S. Government delegate on the final record vote at the ILO stated: "United States law requires a visa for shore leave, joining a ship or transferring to another ship, passing in transit to join a ship in another country, or for repatriation. The seafarers' identity document will not be accepted in lieu of a visa or travel document. Possession of a seafarer's identity document will not guarantee issuance of a visa."

⁵ The question (B4 (a)) reads: "Does the requirement to admit the bearers of seafarers' identity documents for the purposes of shore leave raise any problems for Members?"

This same objective of the U.S. government was reaffirmed at the final vote on the new ILO Convention on June 18, 2003. After having voted in favor of the new Convention, the U.S. government delegate explained that, under U.S. immigration law, the seafarers' identity document would not be accepted *in lieu of* a visa nor would possession of such a document guarantee issuance of a visa to the United States. "Nevertheless, we recognize the special professional needs of seafarers as described in the Preamble to this Convention and we are considering what steps we can take to facilitate the visa application process for them".⁶

The relevance of defining and implementing such steps, using the new seafarers' identification document to establish and verify the identification, employment history and credentials of individual seafarers as part of the visa application process and in facilitating their transit in and out of the United States, is highlighted by recent decisions by the U.S. Department of State concerning the visa application process and requirements for foreign seafarers. The de facto elimination of the so-called crew list visa system will indisputably lead to a significant increase in the already significant waiting times for the issuance of individual seafarers visa at many U.S. diplomatic posts, including in the main seafarer supplying countries in the Southeast Asia.⁷

The impending deadline of December 31, 2003, for the statutorily required entry-exit system ("US VISIT") at U.S. airports and seaports for foreign visitors to the U.S., including seafarers, also highlights the importance of determining the use, which the U.S. government can and will make of the new international seafarers identity document.

In this regard, we understand that the biometric identifiers to be used in the US VISIT program may be different from, and thus incompatible with, those that were included in the new ILO document. If that is true, it would appear to mean that the new identification document could not be used for the expedited processing of foreign seafarers in the US VISIT program. We would appreciate clarity on this issue. The biometric identifiers, we understand, are intended to be the same for the purposes of both the US VISIT program and the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub.L. 107-173). That statute requires that, effective October 2004, foreign visitors to the United States shall only be issued visas or other travel and entry documents with biometric identifiers. It would thus appear that we might be approaching a situation, where incompatible biometric identifiers would prevent the new document from also playing a facilitating role in the visa application process.

Even though we fully recognize that the Coast Guard cannot, and should not, be held accountable for decisions made elsewhere in the government, and even though we recognize that this issue is beyond the scope of this particular rulemaking, we would hope that the agency, within the context of its responsibilities under the MTSA pertaining to foreign seafarers, could assist the industry and its employees understand the issues involved, initiate the needed

⁶ Provisional Record No 27, Twenty-Second Sitting of the 91st International Labor Conference, page 27/10 (accessible at www.ilo.org/public/english/standards/relm/ilc/ilc91/pdf/pr-27.pdf).

⁷ In a cable, dated May 21, 2003, to all U.S. embassies and consulates concerning the elimination of consular officers' discretion to waive the personal appearance requirement for most non-immigrant visa applicants, including for seafarers, the Secretary of State observed that the Department of State "expects and accepts that manned posts will face processing backlogs for the indefinite future" as a result of the new rule.

interagency deliberations on the possible future use of the new document, and clearly explain its uses, whatever they may or may not be, to the industry.

Consideration of Other Organizations Competent in Maritime Security

In the supplemental discussion preceding Part 101 (68 Fed.Reg. 39254-39255), the Coast Guard discusses, amongst other things, the parameters and competencies that should be considered by vessel and facility owners and operators to guide their decisions to hire a company to assist in meeting the requirements of the interim rules and the ISPS Code and SOLAS amendments. The Coast Guard states that, while it may provide further guidance on competencies for maritime security organizations, it does not intend to list such organizations, to provide standards within the regulations, or to certify such organizations. The Coast Guard also states that standards and requirements for armed security guards are included in the above discussion on competencies for evaluating maritime security organizations, and that such standards and requirements are a matter of state and local law, as are the parameters for the legal use of force.

The Coast Guard has previously stated publicly that vessel and facility owners and operators are not only responsible for the hiring of armed security guards, when necessary, but also are liable for the actions of these hired guards. We are therefore concerned that there exist no uniform national guidelines or certification requirements for armed security personnel. We are aware of states that have neither standards nor requirements for the certification or conduct of armed security guards and we are aware of other states that have diverse, inconsistent standards for armed security guards. We believe that because vessel and facility owners and operators can be required pursuant to federal law, to obtain the services of security guards, and sometimes even armed guards (for example, when directed to detain seafarers on board a vessel with armed guards), there should be minimum standards guiding the qualifications, certification and performance of those armed security guards. Without such standards, vessel and facility owners and operators are left in the unwelcome position of being required by the government to hire armed security guards for whom no certification standards exist.

The Coast Guard states (68 Fed.Reg. 39255) that it intends to work with state homeland security representatives to encourage the review of all standards related to armed personnel and the services they provide to the maritime community. We believe it is reasonable and appropriate that the Coast Guard review existing state and local standards for armed guards with a view to developing minimum uniform national guidelines. Perhaps the Coast Guard could promulgate such guidelines as it finalizes its nationally applicable Standard Operating Procedures for handling detained crewmembers in concert with the Bureau of Customs and Border Protection.

We also request that the Coast Guard consider delegating to the AMS Committees the task of developing a list of minimum criteria for the certification and performance of armed security service providers and then evaluating local armed security service providers with a view to publishing a list of companies that meet these criteria. We would also suggest that the results of AMS Committee evaluations of local armed security service providers could be published on the NRC website with appropriate contact information, so vessel and facility owners and operators

can quickly and easily access a list of AMS Committee-approved armed security guard providers.

Foreign Port Assessments (68 Fed.Reg. 39265)

Foreign port assessments are not discussed in any of the temporary interim rules published on July 1. The topic is, however, briefly discussed in the Supplementary Information to the Temporary Interim Rule on Implementation of National Maritime Security Initiatives.

That discussion makes clear that the Coast Guard will be the U.S. government agency with primary responsibility for conducting foreign port assessments. It confirms that the Coast Guard intends to verify foreign port facilities' compliance with SOLAS and the ISPS Code, but that it will be the responsibility of the Contracting Government in whose jurisdiction the foreign port facilities are domiciled to ensure compliance with the international requirements. It is emphasized that the Coast Guard "will work with relevant Contracting Governments to facilitate these evaluations".

Finally, the Supplementary Information also makes clear that the Coast Guard retains the authority to subject those vessels, which have been calling on foreign port facilities that do not meet the SOLAS and ISPS Code requirements, to compliance and control measures, "even if the vessel itself has a valid ISSC and an approved security plan".

It is very important that no confusion exists within industry or vis-à-vis foreign governments as to which U.S. government agency will be primarily responsible for implementing U.S. policies, commitments, obligations and rights under international instruments to which the U.S. is a party. The Coast Guard has traditionally had, and continues to have, a leadership role in the IMO and in setting and developing international standards and requirements in the area of vessel safety and security, including the interface between vessels and port facilities. If anything, that leadership role has only been reaffirmed during the course of the IMO negotiations that resulted in the amendments to SOLAS and approval of the ISPS Code. The Coast Guard has won the respect of the international community, and obtained its leadership role in that community, because of the integrity, sensitivity and professionalism that continues to characterize the service, and how it executes the obligations and rights as a port state to verify calling foreign vessels' compliance with international mandatory commitments and domestic requirements. Foreign port assessments will require the same skills and professionalism.

As stated in the Supplementary Information, each Contracting Government to SOLAS and the ISPS Code has the right and obligation to ensure its port facilities' compliance with the international commitments laid down in those mandatory instruments. Contracting Governments are required to make sure that security assessments are undertaken for their port facilities, and that security plans are developed and approved that address identified vulnerabilities and meet the requirements of the Code. Reputable administrations have the right to expect that other reputable administrations will respect, and trust, that such security assessments and security plans for their port facilities are undertaken with the seriousness and dedication that the fight against terrorism warrants and requires.

One administration's request to be allowed to evaluate another administration's assessments and plans, and the measures required by those plans, could be perceived as an expression of a lack of trust in the integrity and commitment of the host nation to abide by its international commitments, *unless* the requesting administration makes such requests appropriately, conducts the evaluation with the full cooperation and involvement of the host nation, and in accordance with clear, accepted and verifiable criteria, and, shares the results and conclusions of the evaluation with the host nation. Furthermore, a government that requests the ability to evaluate another nation's port facilities must do so in a way that it itself would find acceptable, non-intrusive and non-degrading if the host nation, based on the principle of reciprocity, were to request to evaluate the requesting nation's port facilities.

We are confident that the Coast Guard will pursue its intention to evaluate other nations' port facilities in such a considerate, correct and transparent way. Mindful, however, of the particular interest devoted to this issue during the IMO negotiations and afterwards, we would encourage the Coast Guard to continue to develop a prudent and transparent framework for its foreign port assessments that can be shared, beforehand, with other nations' maritime administrations, and which confirms the Coast Guard's intention to base such assessments on the criteria, standards and principles laid down in the relevant internationally agreed instruments, i.e. SOLAS and the ISPS Code. In this regard, the Council would like to encourage the Coast Guard to reach out to the various nations to fully explain the Coast Guard's policies, intentions and objectives before any foreign port assessments are actually undertaken. Anxiety over the unknown and the unexpected, which may be particularly pronounced when issues of national sovereignty are perceived to be involved, should be avoided if possible. For that reason, and for these purposes, the Coast Guard may also want consider to supplement its outreach efforts to the host nations with an active dialogue with the diplomatic representations in Washington, D.C., of these same nations.

Finally, we noted above that a useful guiding principle for the Coast Guard's pursuit of its intention to evaluate foreign port facilities should be what kinds of requests the United States would find acceptable and legitimate of it from other governments in the area of port facility assessments. We suggest that requests, based on, reflecting and conducted in full accord with the principles, commitments and obligations laid down in SOLAS and the ISPS Code, and which acknowledge and respect the principle of reciprocity, are likely to be deemed bona fide by other reputable administrations.

That guiding principle should also, we believe, be applied to the control and compliance measures that could be taken against vessels, which have called on foreign port facilities that are deemed not to meet the internationally agreed commitments and obligations. We would therefore encourage the Coast Guard, in the final rule, to amend the language of 33 CFR § 101.410 (d) so that it better reflects the conclusion of the discussion in the Supplementary Information, i.e., that vessels may be subject to control and compliance measures if they have called "on foreign port facilities that do not meet the requirements of SOLAS and the ISPS Code".⁸ We would also encourage the Coast Guard, to the extent possible, to develop and include in its Port State Control Regime guidelines for what such vessels would be expected to do to satisfy any security

⁸ A similar formulation is used in the discussion at 68 Fed.Reg. 39243 ("...and any control measures that may be required when [vessels] call on foreign port facilities that do not comply with SOLAS and the ISPS Code").

concerns the Coast Guard may have, and to generally follow the transparent, well-known and internationally accepted processes and procedures for boarding and inspection of vessels under the Port State Control Regime. Lastly, in the event that the Coast Guard determines, after performing the assessments as discussed above, that any foreign port facilities have been deemed not to meet the requirements of the SOLAS and ISPS Code, we would encourage the Coast Guard to make such information publicly available, preferably on the Coast Guard's Port State Control website, so that shippers, consignees, ship operators and carriers – before arriving at the U.S. port – can proactively address any security concerns.

Vessel and Facility Security Plans For Handling Approaching Recreational Vessels

The supplemental discussion of the Coast Guard's National Risk Assessment Tool (N-RAT), which precedes Part 101 of this interim rule (68 Fed.Reg. 39250), discusses, among other things, the necessity for security plans to include provisions for how a vessel or facility would respond to approaching recreational vessels that may reasonably pose a threat. The results of the N-RAT indicate, however, that recreational vessels pose the lowest relative risk of being involved in a transportation security incident of all of the vessel and facility types evaluated by the tool.

It is unreasonable to expect a facility or a commercial vessel, while underway or in port, to exert control of the waters around the vessel or facility and to prevent an unannounced attack by a recreational vessel. Identifying an ill-intentioned recreational vessel out of the hundreds of recreational vessels that operate each day near vessels and port facilities would be impossible, unrealistic and impractical. But more importantly, such a requirement imposes on the vessel or facility a law-enforcement or policing role that is as inappropriate as it is unpredictable.

Similarly, while it is unreasonable to expect vessels and facilities to deploy countermeasures to stop or deter a recreational vessel intending to damage the vessel or facility, it is reasonable for vessels and facilities to be aware of and report suspicious activities of recreational vessels. The most appropriate action for a vessel or facility upon witnessing suspicious activity by a recreational vessel would be to immediately notify the Coast Guard and the local law enforcement authorities.

We believe that inclusion of requirements for private facilities and international vessels to police public waterways is clearly outside the scope of privately owned companies' authority and competence. These activities are, and should remain, activities undertaken by the U.S. Coast Guard and other law enforcement agencies.

Changes to Cost Assessment Summary

While we appreciate the Coast Guard's efforts to amend the initial cost estimates published in the December 20, 2002 Maritime Security Notice, we note that the Coast Guard's amended cost estimates still do not include the estimated costs for foreign-flag SOLAS vessels that operate in U.S. waters. Foreign liner vessels that call on U.S. ports make up a significant part of the regulated community under this security initiative.

III. Area Maritime Security (Part 103)
(Docket Number: USCG-2003-14733)

Composition of an Area Maritime Security (AMS) Committee (Section 103.305)

With regard to the composition of AMS Committees, we believe it is important that government agencies that have roles in maritime and cargo security be involved in the AMS Committee membership. In particular, we recommend that the Coast Guard ensure that local port representatives from CBP are present on the AMS Committees to ensure adequate coverage not only of vessel and port facility security issues, which are under the purview of the Coast Guard, but also of cargo security issues, which are under the purview of CBP.

As discussed in detail in the above comment entitled, “Consideration of Other Organizations Competent in Maritime Security”, we also recommend that the Coast Guard consider delegating to all AMS Committees the tasks of 1) developing a list of minimum standards for the certification and performance of armed security service providers, and 2) evaluating armed security service providers within the Area with a view to publishing a list of companies that meet these criteria on the NRC website.

IV. Vessel Security (Part 104)
(Docket Number: USCG-2003-14749)

Introductory Vessel Security Comments

The Council commends the Coast Guard on its development of meaningful and internationally consistent security requirements for vessels that operate on the waters of the United States. The vessels operated by the liner shipping industry are deployed in regularly scheduled service to and from the major U.S. container, roll-on roll-off and car carrier facilities. Liner vessels will typically call at the same U.S. ports, often with the same crewmembers aboard, many times a year on their service routes, and are generally well known to the U.S. Coast Guard and to CBP. The liner shipping industry depends on its ability to provide reliable, regular, and on-time scheduled service to American importers and exporters. The operational delays and costs that liner vessels--and consequently America's importers and exporters--could face if they are deemed not to be in compliance are substantial. Accordingly, it is critically important that the regulations affecting the liner shipping industry be precise, transparent, and uniformly applied. The Council fully supports the Coast Guard's recognition of the SOLAS and ISPS Code provisions that vessels' Vessel Security Plans are to be approved by the respective flag administrations or designated Recognized Security Organizations. We also fully recognize and support the Coast Guard's declared intention to use appropriate port state control to ensure that the new security requirements are and urge that this process be clear, transparent, and uniform across U.S. ports as well.

Applicability (Section 104.105)

The Council and its members strongly support the Coast Guard's plan to deem flag administration approval of foreign ship security plans to constitute approval under 46 U.S.C. section 70103, provided the vessel security plan complies with the SOLAS amendments and ISPS Code, Part A, having taken into account the relevant provisions of ISPS Code, Part B. To that end, we also support the Coast Guard's plan to deem possession of a valid International Ship Security Certificate (ISSC) to be proof of a foreign vessel's compliance with the SOLAS amendments and ISPS Code, and thus with U.S. requirements.

The fundamentals of international comity, the mechanics of the SOLAS Convention, and the Coast Guard's international obligations under SOLAS and the ISPS Code, necessitate that flag state administrations be responsible for approving and certifying their vessels' compliance with the mandatory international instruments. The ISPS Code and SOLAS amendments rely on a tacit approval process by which Contracting Governments that are already signatories to the SOLAS Convention, such as the United States, are deemed to be in concurrence with the requirements of the ISPS Code and SOLAS amendments unless they have specifically refuted acceptance of the new Convention by the July 1, 2004 entry into force date. In that regard, silence on this issue is equivalent to agreement with and approval of the Convention.

Furthermore, the U.S. Congress expressed its intent on this matter in paragraph 15 of Section 101 of the MTSA, which states: "The International Maritime Organization and other similar international organizations are currently developing a new maritime security system that contains the essential elements for enhancing global maritime security. Therefore, it is in the best interests of the United States to implement new international instruments that establish such a system."

All of these points taken together clearly buttress the Coast Guard's decision to rely on flag administration approval of a foreign vessel security plan to establish compliance with the ISPS Code and SOLAS amendments and the relevant provisions of the vessel security interim rules.

Port State Control Program

In the supplemental discussion section preceding the interim rules in Part 104 (68 Fed.Reg. 39297) the Coast Guard states that it will use its Port State Control program to verify that foreign SOLAS vessels have an approved Vessel Security Plan (VSP) that fully complies with SOLAS and the ISPS Code, and thereby meets the requirements of Part 104. The Coast Guard further states that noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port and/or significant delay.

The Council recognizes that the Coast Guard retains its Port State Control authority to ensure that all foreign vessels calling on U.S. ports are in compliance with the ISPS Code and SOLAS amendments. At the same time, we expect that the Coast Guard will continue to implement its Port State Control authority in a transparent and predictable way with a high degree of uniformity and coordination between and amongst COTP areas.

Additional details regarding the Coast Guard's Port State Control program and vessel targeting matrix are provided in the supplemental discussion preceding the interim rules in Part 101 (68 Fed.Reg. 39243). In this section, the Coast Guard states that a vessel's or port facility's history of compliance or lack thereof will be important factors in determining the appropriate measures to ensure maritime security. Furthermore the Coast Guard states that the performance of the owner, operator, flag administration, RSO, charter or port facility with regard to maritime security will also be factored into the targeting matrix and will affect the decision as to what enforcement actions, if any, the Coast Guard will take.

The Council supports the Coast Guard's use of a targeting matrix into which specific risk factors are input in a transparent and consistent way so that an appropriate and timely Port State Control enforcement decision can be made in advance of the Port State Control inspection. We believe that such a targeting matrix could become a useful tool that would enable to Coast Guard to ensure for a uniform, coordinated Port State Control approach in which compliance is rewarded by lower risk scores and consequently by a reduced risk of being boarded, and in which lack of compliance would be quickly identified. We recommend, however, that the Coast Guard maximize national consistency and transparency with regard to the factors that are evaluated in the targeting matrix. This would enable industry to work alongside the Coast Guard in identifying and addressing maritime security risk factors.

Alternative Security Program (Section 104.140)

While this provision in Part 104 of the interim rules does not specifically allow for the designation of an approval process for Alternative Security Programs for international vessels, we recommend that the Coast Guard consider use of the International Chamber of Shipping (ICS) model ship security program, which includes a model ship security plan, security assessment guidelines, and a model training program for ship security personnel, as a positive factor in evaluating U.S. bound vessels for targeting. The ICS model ship security program has been developed and reviewed in cooperation with several international registries and shipping associations.

Vessel Security Plans in English

In the supplemental discussion preceding Part 104 (68 Fed.Reg. 39297), the Coast Guard states that if, during an expanded examination, those sections of the VSP the port state is allowed to review are not written in English, a vessel may be delayed while translator services are acquired. The Council understands that Coast Guard Port State Control officers may be delayed when they encounter a foreign VSP written in either French or Spanish (the other two authorized languages for VSPs according to SOLAS), and that—in order to avoid such delays—vessels should be encouraged to carry a copy of their VSP written in English. Such a recommendation should explicitly be included in Part 104.

Security Training For All Other Vessel Personnel (Section 104.225)

This provision requires that all other personnel aboard the vessel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or experience, the following five security provisions: 1) relevant provisions of the VSP, 2) the meaning and requirements of the different MARSEC levels, 3) detection of dangerous substances and devices, 4) recognition of threatening behavioral patterns and characteristics, and 5) techniques to circumvent security measures. This requirement would effectively mandate, for example, that a contractor that comes on board the vessel for 30 minutes to repair a loose wire, would be required to receive training on the above five subjects. Complying with this requirement would be extremely burdensome and would make it exceedingly difficult for liner vessels, which are in port only long enough to unload and reload the ship, to perform routine shipboard maintenance and repairs. Such a rigid requirement goes beyond what is needed to enhance maritime security.

The Council therefore recommends that the Coast Guard eliminate this requirement for persons who are not ship's crew, and replace it either with similar recommendatory guidelines, or institute a minimum time onboard threshold, such as 24 hours, after which all vessel security personnel would be required to receive security training.

Declarations of Security (Section 104.255)

According to section 5.1 of Part A of the ISPS Code, "Contracting Governments shall determine when a Declaration Of Security (DOS) is required by assessing the risk the ship/port interface or ship-to-ship activity poses to people, property or the environment." The DOS provision within this Part is one of four provisions within the vessel security interim rules that all foreign SOLAS vessels must comply with.

With respect to vessel-to-vessel interface, at MARSEC levels 2 and 3, a DOS must be signed prior to any vessel-to-vessel interface. This requirement would be particularly troubling when a liner vessel is enroute the facility and requires pilot and tug assistance. According to this requirement, the pilot boat operator and the tug operator would have to cease operations, hold a meeting in which security roles and responsibilities were discussed, sign a DOS and then resume vessel operations. Liner vessels as well as tug and pilot boats cannot safely loiter in the middle of a busy harbor area to facilitate the signing of a DOS. In this instance, the signing of the DOS could create an unsafe navigational situation.

We therefore urge the Coast Guard to amend its MARSEC level 2 and 3 DOS requirements as follows: Regarding vessel-to-vessel interface, waive the DOS requirement except in cases where the duration of the interface will exceed three hours.

Paragraph (e) of this section states that at MARSEC levels 1 and 2, VSO's of vessels that frequently interface with the same facility may implement a continuing DOS for multiple visits, provided that the effective period of the DOS does not exceed 90 days at MARSEC 1 and 30 days at MARSEC 2. The Council believes that in cases where a continuing DOS is warranted, it would be more appropriate to waive the DOS requirement and to instead include the measures

that would have been detailed in the continuing DOS in the VSP and FSP, as appropriate. The premise on which a DOS is based is that the terms of the DOS are temporary and that the agreements in the DOS are to be used to address immediate security arrangements. Once arrangements have been made that will take effect for, perhaps 30 days or more, or would be done during future multiple visits, those arrangements should more appropriately be entered into the VSP and FSP and the requirements for a DOS between the two parties should be waived.

We would also like to recommend that in such cases where a continuing DOS is warranted, the maximum effective period must be longer than 90 days for MARSEC 1 and 30 days for MARSEC 2 for the value of the continuing DOS to be realized. We suggest that these effective periods be amended to 360 days for MARSEC 1 and 90 days for MARSEC 2.

Vessel Requirements for Waterborne and Waterside Security and Underwater Screening

Section 104.240 (e) *MARSEC Level Coordination and Implementation*, and Section 104.265 (f) (6), *Security Measures for Access Control*, include multiple requirements at MARSEC levels 2 and 3 that are of concern to us. These requirements would require vessel owners and operators to make arrangements for, “waterborne security patrols”, “screening the vessel for the presence of dangerous substances and devices underwater” and “detering waterside access to the vessel, which may include...providing boat patrols.”

Enforcing waterside security in U.S. waters is inherently a government function that must be performed by a duly authorized government law enforcement officer—not by the crew of a vessel. Policing the waters adjacent to a vessel or facility (whether the vessel is in port or piloting restricted waterways) is a function that is clearly outside the scope of a shipping company’s competence and authority and would create challenging legal questions with regard to use of force guidelines and liability. Vessels transporting cargo to and from U.S. ports have no control, competence or authority over U.S. navigable waterways or the persons on them. The responsibility for patrolling waterways around vessels and private port facilities is and should remain the sole responsibility of federal, state, and local law enforcement authorities.

We strongly urge the Coast Guard to amend these interim rules, and any other such references, to remove any provisions that require vessels or facilities to perform waterside security patrols.

Vessel Plan Security Measures for Handling Cargo (Section 104.275)

The Council has a number of comments on this section of the rulemaking.

The liner shipping industry has worked closely with the U.S. government to address the security issues arising with the transportation of sealed cargo containers in international trade. The Council has supported the “24-hour rule”, pursuant to which the government is provided the advance cargo shipment information 24 hours before a container is loaded aboard a vessel bound for the U.S. in the foreign port of loading. Customs and Border Protection (CBP) screens the

information regarding every such container bound for the United States using its Automated Targeting System. If any such container doesn't meet the government's risk assessment criteria, CBP can order the carrier not to load the container onto the vessel at the foreign port of loading, can work with the foreign customs authorities to inspect the container at the port of loading, or can order the container held and inspected at the U.S. port of discharge.

The Council has supported this strategy as well as the government's Container Security Initiative, pursuant to which the United States and the customs authorities of our trading partners agree to cooperate in sharing information, in conducting risk analysis, and in inspecting any containers that warrant inspection. Originally, 20 "mega-ports" (defined in terms of their export container volume to the United States) were identified as being eligible for CSI status. Together with the three Canadian ports that under a separate, bilateral agreement became CSI operational a little over a year ago, these ports make up Phase I of the CSI initiative. Their current status is as follows:

- 15 ports are CSI operational: Halifax, Montreal, Vancouver, Rotterdam, Le Havre, Bremerhaven, Hamburg, Antwerp, Singapore, Yokohama, Hong Kong, Felixstowe, Genoa, La Spezia, and Gothenburg (a Phase II port – see below)
- Next in line to become CSI operational: Pusan and Algeciras
- No firm time line for when to become CSI operational: Kobe, Nagoya, Tokyo, Shanghai, Shenzhen, Laem Chabang, Port Klang and Tanjung Pelepas (these two are Phase II ports – see below)
- CSI agreement not yet signed with host government: Kaohsiung.

CBP opened Phase II of the CSI initiative by signing agreements earlier this year with Sweden and Malaysia, respectively. On June 25, an agreement was signed with Sri Lanka Customs for the port of Colombo. On July 17, an agreement was signed with South African Revenue Service for the port of Durban.

Between 11-13 additional European ports are expected to become CSI ports during phase II, and Customs Commissioner Bonner has publicly stated that an additional 10 ports or so in other parts of the world may be covered by Phase II, including ports in Turkey and Dubai. CBP is also talking with the U.S. Department of State on the possibilities of including Latin American ports in this phase.

The Council and its member companies have also supported Customs' Trade Partnership Against Terrorism (C-TPAT). Every member Company of the Council is a participating C-TPAT Sea Carrier.

The industry has strongly supported the creation and implementation of this security infrastructure and capability, because it recognizes that trading nations' governments must have a security profiling and container inspection capability that: 1) allows their Customs authorities to profile and screen shipments to prevent security threats from being shipped in containers,

2) can be integrated with other government intelligence capabilities, and 3) can immediately be adjusted to provide enhanced measures in the event that there is a security incident and the public demands higher security scrutiny for trade to continue flowing.

The necessary operating characteristic of liner shipping is that the vessel operator receives a sealed container from the shipper. It does not load (or “stuff”) the container. It does not break the seal the shipper applies to the container, and it does not inspect the cargo contents of the container. Containerized cargo moves under seals. Accordingly, the security measures for handling cargo must reflect the fact that the carrier does not actually handle the cargo itself, but handles a sealed container.

The Interim Rule’s treatment of container cargo handling goes beyond the terms of the ISPS Code and raises issues that are being addressed through other agencies and programs within the Department of Homeland Security. We wish to ensure that these rulemakings do not establish inconsistent or duplicative measures for addressing container cargo security. Specific comments on the Interim Regulations addressing these concerns follow.

Section 104.275(a)(5): This section provides that “the vessel owner or operator must ensure that security measures relating to cargo handling... are specified in order to coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures”. We do not understand what this anticipates or would require. It is clear that containerized cargo security is a shared responsibility. The shipper is responsible for the secure loading or “stuffing” of a container and the application of a high security seal to the container upon conclusion of the container stuffing process. The transport operator or facility operator is responsible for the security of the container while it is in its custody. While the vessel operator and the facility will have established security procedures for handling containerized cargo, there will not as a matter of generally applicable commercial conduct be a security procedure agreement between a vessel operator and a shipper. Some types of cargo might justify agreed security procedures with a shipper, but the vast majority of containerized cargo does not. It is not clear what such an established agreement or procedures would address or when it would be necessary to address it. We urge the final rule to clarify that this provision is not mandatory, and that compliance with government security regulations is adequate for this purpose.

Section 104.275(a)(6): This section requires that “the vessel owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the facility, are specified in order to be able to *check cargo for dangerous substances and devices at the rate specified in the approved Vessel Security Plan. Means to check cargo include: (i) Visual examination; (ii) Physical examination; (iii) Detection devices such as scanners; or (iv) Canines.*”

As stated above, vessel operators do not open sealed containers and they do not and cannot conduct a visual or physical examination of a container’s cargo, unlike some bulk or break bulk cargoes that can be seen during the vessel loading process. Second, vessel owners do not own or operate container scanning or inspection devices, and such equipment cannot be operated aboard a vessel. Further, the stevedore and terminal operators that load the industry’s vessels do not own or operate such scanning equipment. Such equipment is owned and operated by

government Customs agencies, as is explicitly recognized in the various CSI agreements.⁹ Container scanning and physical examination of containerized cargo is a recognized government function, not a vessel operator or terminal operator function. In the same vein, vessel operators do not possess dogs, although again CBP has an entire federal program of dogs trained to detect certain substances. Third, because of the 24-hour rule and the CSI agreements, it is the government, not the vessel operator, that will determine “the rate” of container inspections.

Vessel operators should not be expected to conduct container screenings and inspections. This is a law enforcement function, and vessel operators do not have the risk assessment screening software or hardware, the agreements with foreign Customs administrations, the government intelligence functionality, the equipment or training, or the commercial latitude to determine when their customers’ containers must undergo the expense and delay of inspection.

Accordingly, it is essential that the Final Regulations clarify that a carrier fulfills cargo screening and inspection obligations for handling containerized cargo if its plan, in coordination with the facility operator, provides for routine checking of containers, files the required advance containerized shipment data in a timely manner before vessel loading with CBP, does not load any container for which CBP has issued a “do not load” message, and delivers as directed any container that CBP wishes to inspect or scan either at the foreign port of loading or the U.S. port of discharge.

Section 104.275(b): This section addresses MARSEC Level 1 cargo handling requirements. We do not object to this subsection’s provisions, but have two comments.

First, paragraph (1) requires a vessel operator to “routinely check cargo”. For containerized cargo, we note that the vessel operator would be checking the container, not the cargo per se.

Second, we note the obligation to implement measures to: “Check, in liaison with the facility, seals or other methods used to prevent tampering” (Sec. 104.275(b)(4)). We believe any carrier that is a Sea Carrier C-TPAT participant should be considered having met this plan obligation.

The Council recognizes that this issue would benefit from a more specific, required protocol, and it will be working with officials in other parts of the Department of Homeland Security with the objective of establishing more specific requirements pursuant to sections 111 and 70116 of the Maritime Transportation Security Act.

Section 104.275(c): This section addresses MARSEC Level 2 cargo handling requirements. We have two comments on this subsection.

First, paragraph (5) requires the vessel operator to consider “increasing the frequency of the use of scanning/detection equipment”. As discussed above, the decision to use and the frequency of use of scanning/detection equipment is a government function, not a vessel operator function. It is entirely appropriate to expect a vessel or marine terminal operator to abide by government directives to deliver the appropriate containers to the appropriate place and persons for

⁹ One of the required terms of Container Security Agreements is that the foreign government must assure the availability of non-intrusive inspection equipment and radiation detection equipment that can be utilized for inspections when deemed warranted.

inspection, but those inspection decisions and the use of the equipment will be the government's, not be the vessel operator's. We request that the Final Regulation make this clear.

Second, paragraph (6) again requires enhanced security measures pursuant to an agreement with the shipper or other responsible party. As discussed above in the comments to section (a)(5), there may or may not be such coordinated measures, and we request that the Final Regulation make it clear that such agreements are not mandatory.

V. Facility Security

(Docket Number: USCG-2003-14732)

Security Training for All Other Facility Personnel (Section 105.215)

Consistent with the Council's comments on Section 104.225 regarding security training for all other personnel aboard vessels, this requirement would appear to be equally superfluous when applied to facilities. The Council therefore recommends that the Coast Guard eliminate this requirement, replace it with recommendatory guidelines, or institute a minimum time onboard the facility threshold, such as 24 hours, after which all facility security personnel would be required to receive this training.

Declarations of Security (Section 105.245)

The DOS requirements for facilities are essentially identical to those already discussed in the Council's comments on Section 104.255. We recommend that the Coast Guard amend the vessel-to-facility and vessel-to-vessel DOS requirements as outlined in our comments on Section 104.255.

Facility Requirements for Waterborne and Waterside Security and Underwater Screening

Similar to the Council's comments in Part 104, Sections 104.240 (e) and 104.265 (f), the interim rule in Part 5, Section 105.230 (e), *MARSEC Level Coordination and Implementation*, and Section 105.255 (f), *Security Measures for Access Control*, include vexing requirements in which facility owners and operators would be required to make arrangements for the use of "waterborne security patrols", "examination of piers, wharves, and similar structures...for the presence of dangerous substances and devices underwater" and "deterring waterside access to the facility, which may include...using waterside patrols."

Again, enforcing waterside security in U.S. waters is inherently a government function that must be performed by a duly authorized government law enforcement officer—not by the staff of a private marine terminal. Policing the waters adjacent to facility (whether the vessel is in port or piloting restricted waterways) is a function that is clearly outside the scope of a facility operator's competence and authority and would create challenging legal questions with regard to use of force guidelines and liability. Private cargo facilities have no control, competence or

authority over U.S. navigable waterways or the persons on them. The responsibility for patrolling waterways around private port facilities must remain the sole responsibility of federal, state, and local law enforcement authorities.

We strongly urge the Coast Guard to amend these interim rules, and any other such references, to remove any guidance that suggests that facilities should perform waterside security patrols or conduct underwater security screening.

Facility Plan Security Measures for Handling Cargo (Section 105.265)

Consistent with the Council's comments on Section 104.275 regarding containerized cargo handling, some of the same issues arise in this section.

Section 105.265(a)(8): This provision would require the facility to "coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures." While the facility and the vessel operator may have established security procedures, there will not be, as a matter of normal commercial conduct, a security procedure agreement between a facility and a shipper. This provision should not be mandatory.

Section 105.265(a)(10): This provision would require a U.S. facility to have the capability to "be able to check cargo entering the facility for dangerous substances and devices at the rate specified in the approved Facility Security Plan (FSP). Means to check cargo include: (i) Visual examinations; (ii) Physical examinations; (iii) Detection devices, such as scanners; or (iv) Canines."

As stated above, vessel and terminal operators do not open sealed containers and thus cannot conduct a visual or physical examination of a container's cargo, unlike some bulk or break bulk cargoes that can be seen during the vessel loading process. Second, facility operators do not own or operate container scanning devices. Such equipment is owned and operated by CBP at container inspection facilities around the country. Container scanning and physical examination of containerized cargo is a recognized government function, not a vessel operator or terminal operator function. CBP has spent in excess of \$200 million on non-intrusive container inspection equipment in the last two years and will be spending more money on this technology in the future, as it expands its cargo-screening infrastructure. Third, because of the 24-hour rule and CBP's screening of every container shipment, it is the government, not the vessel operator, that will determine "the rate" of container inspections. Finally, U.S. facility operators do not have dogs trained to inspect cargo; CBP does.

Facility operators should not be the parties that are expected to conduct these container screenings and inspections. This is a law enforcement function, and they do not have the risk assessment screening software or hardware, the government intelligence functionality, the equipment or training, or the commercial latitude to determine when a shipper's container must undergo the expense and delay of inspection.

Accordingly, we believe it is essential that the Final Regulations clarify that a facility fulfills cargo screening and inspections obligations for handling containerized cargo if it routinely

checks containers for evidence of tampering, and, working in conjunction with the vessel operator, does not load any container for which CBP has issued a “do not load” message, and delivers to the designated place and party, as directed by government officials, any container that CBP wishes to inspect or scan.

Section 105.265(b): This section addresses MARSEC Level 1 cargo handling requirements. We do not object to this subsection’s provisions, but have two comments that are the same as those above on the MARSEC Level 1 comments for vessel plans.

First, paragraph (1) requires a facility to “routinely check cargo”. For containerized cargo, we note that the facility would be checking the container, not the cargo per se.

Second, we note, however, that the obligation to implement measures to “check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility”. The Council recognizes that this issue would benefit from a more specific, required protocol, and it will be working with Department of Homeland Security officials with the objective of establishing more specific requirements pursuant to sections 111 and 70116 of the Maritime Transportation Security Act.

VI. Automatic Identification System; Vessel Carriage Requirement (Part 164)
(Docket Number: USCG-2003-14757)

Automatic Identification System (Section 164.46)

The Council supports the Coast Guard’s affirmation of the internationally agreed compliance dates set forth in SOLAS. This reflects and underpins the international obligations agreed to in SOLAS, and will be conducive to greater international consistency and uniformity.

The Coast Guard is reportedly behind schedule in its AIS implementation strategy and is currently working to build the necessary infrastructure to rollout its AIS systems at existing Vessel Traffic Service (VTS) centers over the next two years. Our primary concern is that existing SOLAS vessels of greater than 50,000 gross tons, which comprise most of the vessels within the Council’s Membership, will be required to have installed operational AIS systems by July 1, 2004—before the Coast Guard has even completed its AIS installations at existing VTS locations. We are concerned that slow roll out of AIS by the United States will send a message to other SOLAS signatories that the AIS implementation deadlines for Contracting Governments are not critical and may be allowed to slip. We urge the Coast Guard to expedite its AIS implementation timelines to the maximum extent possible. There are two additional concerns. One pertains to the utility of a system that is not fully functional. The other relates to equitability, i.e. the need for having a reasonable balance and relationship between the obligations imposed on industry and the commitments the government makes for itself. That balance seems to be lacking in the current AIS deployment plans of the Coast Guard.

VII. Conclusion

The Council appreciates the opportunity to submit comments in response to the Coast Guard's Maritime Security Interim Rules. We fully recognize and appreciate the tremendous effort that the Coast Guard has demonstrated to develop harmonized, meaningful and timely international and domestic maritime security requirements. The Coast Guard's strategy for developing and implementing uniform international and domestic regulations is an excellent model that enhances international maritime transportation security and increases maritime domain awareness. The Council and its Members appreciate the opportunity to support the efforts the Coast Guard and other federal agencies to implement meaningful, transparent and predictable requirements that will enhance the safety and security of America's international commerce, while facilitating the movement of legitimate trade.

Appendix A**WORLD SHIPPING COUNCIL
MEMBER LIST**

- APL
- A.P. Moller-Maersk Sealand (including Safmarine and Torm Lines)
- Atlantic Container Line AB
- CP Ships Holdings, Inc. (including Canada Maritime, CAST, Lykes Lines, Italia Lines, Contship Containerlines, TMM lines, and ANZDL)
- China Ocean Shipping Company (COSCO)
- China Shipping Group
- CMA-CGM Group
- Compania Sud-Americana de Vapores (CSAV)
- Crowley Maritime Corporation
- Dole Ocean Cargo Express
- Evergreen Marine Corporation Ltd. (including Lloyd Triestino and Hatsu Marine)
- Great White Fleet, Ltd.
- Hamburg Sud (including Columbus Line and Alianca)
- Hanjin Shipping Company, Ltd.
- Hapag-Lloyd Container Linie GmbH
- HUAL AS
- Hyundai Merchant Marine Company, Ltd.
- Italia Line
- Kawasaki Kisen Kaisha Ltd. (K Line)
- Malaysia International Shipping Corporation (MISC)
- Mediterranean Shipping Company, S.A.
- Mitsui O.S.K. Lines
- NYK Line
- Orient Overseas Container Line, Ltd.
- P&O Nedlloyd Limited
- United Arab Shipping Company
- Wan Hai Lines Ltd.
- Wallenius Wilhelmsen Lines
- Yangming Marine Transport Corporation, Ltd.
- Zim Israel Navigation Company, Ltd.